Cooperative Efforts To Shut Down Virut Botnet

spamhaus.org/news/article/690/cooperative-efforts-to-shut-down-virut-botnet

During the past few weeks, Spamhaus has worked hard to shut down a botnet called "Virut".

Virut take down
Virut is a worm that spreads through removable drives such as USB sticks and network shares, but it also has file infection capabilities it uses to spread itself. Virut was first detected in 2006 and became a serious threat with an estimated size of more than 300,000 compromised computers. Cybercriminals are using several dozen domain names, mainly within the .pl ccTLD (Poland), but also within the .ru ccTLD (Russia) and the .at ccTLD (Austria). These domains are registered by the operators of Virut to control the botnet. In the past few months, Virut has started to drop ZeuS (ebanking Trojan) and Kehlios (Spambot) onto computers infected with Virut as part of their Pay Per Install business model (PPI).

Due to Virut's persistence, there have already been a couple of take down efforts in the past. However, none of those efforts have been successful thus far. The most recent take down effort was in December 2012, wherein Spamhaus managed to have suspended all the Virut domain names registered through various Polish registrars within the .pl ccTLD. Unfortunately, the Virut botnet gang managed to get the malicious botnet domain names moved to a new registrar called home.pl quickly.

In past few days, Spamhaus has been in close contact with the sponsoring registrar (home.pl), the Polish Computer Emergency Response Team (CERT.pl) to get the domain names suspended. In cooperation with the Polish CERT and the registrar home.pl, we managed to get all the Virut domain names within the .pl ccTLD sinkholed.

In addition, Spamhaus reached out to the Austrian CERT and the Russian based Company *Group-IB* CERT-GIB to shut down the remaining Virut domains within the .at and .ru ccTLDs. In cooperation with Spamhaus, and due to the evidence and intelligence provided by Spamhaus, CERT-GIB was able to shut down all the Virut domains within the .ru ccTLD within a few hours.

The last remaining stronghold for the Virut C&C domains is the .at ccTLD. Having alerted both nic.at and the Austrian CERT multiple times about this issue we hope that they can soon follow the examples set by the work done with .pl and .ru.

The important role of registries and registrars
The Virut takedown effort clearly illustrates the important and meaningful role registries and registrars can play in the fight against cybercrime in general. Domains often are a critical part of malicious infrastructure and by being proactive their efforts can contribute a lot to online

safety. We therefor urge registries and registrars to add clauses to the registration contracts that allow them to take action in cases where the domains involved are clearly only used for bad purposes.

International cooperation to address cyber-threats

How long the shut-down of Virut will last this time is unknown. However, we remain committed to continue the fight against cyber threats. The recent Virut take down is a good model for the future: the internet has no borders, and the community can only fight cybercrime successfully with international cooperation and coordination. Spamhaus will continue to work with its partners around the globe to follow its mission, protecting internet users from cyber threats.

Further reading

CERT.pl: NASK shuts down dangerous Virut botnet domains
Symantec: Snapshot of Virut Botnet After Interruption
Symantec: W32.Virut
Microsoft: Win32/Virut